



Release Notes

FortiSwitchOS 7.4.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



June 2, 2023

FortiSwitchOS 7.4.0 Release Notes

11-740-882418-20230602

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models	5
What's new in FortiSwitchOS 7.4.0	6
GUI changes	6
CLI changes	6
GUI and CLI changes	7
REST API changes	8
Special notices	9
Zero-touch management	9
By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later	9
Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported	9
Downgrading your FortiSwitchOS version requires converting the admin password format first	9
Connecting multiple FSR-112D-POE switches	10
Upgrade information	11
Product integration and support	12
FortiSwitchOS 7.4.0 support	12
Resolved issues	13
Known issues	15

Change log

Date	Change Description
June 2, 2023	Initial release for FortiSwitchOS 7.4.0

Introduction

This document provides the following information for FortiSwitchOS 7.4.0 build 0767.

- [Supported models on page 5](#)
- [Special notices on page 9](#)
- [Upgrade information on page 11](#)
- [Product integration and support on page 12](#)
- [Resolved issues on page 13](#)
- [Known issues on page 15](#)

See the [Fortinet Document Library](#) for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.4.0 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048E, FS-T1024E
FortiSwitch 3xxx	FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D, FSR-424F-POE

What's new in FortiSwitchOS 7.4.0

Release 7.4.0 provides the following new features.

GUI changes

- The *System > Dashboard* page has been reorganized to focus on the operational status of the FortiSwitch unit. In addition, there are now graphs for both the last day and last week of the switch's CPU usage, RAM usage, and temperature.
- The charts for port and interface traffic and packet losses have been enhanced.
- The Route Monitor (*Router > Monitor > Routing*) and IPv6 Route Monitor (*Router > Monitor > IPv6 Routing*) now display the routes graphically, as well as in a table. When you hover your cursor over a route, the route is highlighted, and the destination and interface of the route are displayed.
- You can now add a peer user in the GUI.
- The *Switch > Monitor > 802.1x Status* page is now the *Switch > Monitor > 802.1x > Interfaces* page.
- There is now a separate *Switch > Monitor > 802.1x > Sessions* page that displays the 802.1x MAC authenticated sessions. In the *Sessions* page, you can search for partial or complete MAC addresses. You can also select one or more MAC addresses and de-authorize the clients at those MAC addresses.
- The GUI now provides OS image signature verification.
 - If you upload an unverified firmware image, the GUI displays a "WARNING: This firmware failed signature validation." message.
 - If you log in to a FortiSwitch unit running an unverified firmware image, the GUI displays an "Unverified Image Detected" message.
 - After you log in to a FortiSwitch unit running an unverified firmware image, the GUI displays a triangle with a red exclamation mark in the title bar.

CLI changes

- You can now use the Border Gateway Protocol (BGP) Ethernet Virtual Private Network (EVPN) with Virtual Extensible LAN (VXLAN).
- ARP/ND suppression is now supported for BGP EVPN.
- The FSR-112D-POE, FSR-124D, FS-1xxE, and FS-1xxF models now support IPv6 router advertisement (RA) guard.
- You can now back up the FortiSwitch configuration or logs to a Secure File Transfer Protocol (SFTP) server. You can also restore the FortiSwitch configuration or firmware from an SFTP server. You can use an IPv4 address, IPv6 address, or fully qualified domain name (FQDN) to specify the SFTP server.
- You can now specify in the CLI that the access control list (ACL) prelookup policy applies to all ingress interfaces. Previously, you could specify only a single interface.
- The Message-Authenticator attribute is now used for authentication in MAC authentication bypass (MAB) Access-Request messages.
- The new `get system interface vlan` command lists information about the VLAN interfaces.
- The new `get system interface vxlan` command lists information about the VXLAN interfaces.

- As part of the existing support for RFC 2233, the following counters have been added:

- ifInOctets
- ifInUcastPkts
- ifInErrors
- ifInDiscards
- ifOutOctets
- ifOutUcastPkts
- ifOutErrors
- ifOutDiscards

NOTE: The link status and duplex status are available on all platforms. Some statistics are not tracked (.dot3StatsLateCollisions, .dot3StatsExcessiveCollisions, and .dot3StatsSymbolErrors). Some statistics (.dot3StatsFCSErrors, .dot3StatsDeferredTransmissions, and .dot3StatsFrameTooLongs) are supported only on the following switch models: FSR-124D, FSR-424F-POE, 200 Series, FS-4xxE, 500 Series, FS-1xxxD, and FS-1xxxE.

- EAP-FAST is now supported.
- LACP fallback mode is now supported in the CLI. LACP fallback mode allows a selected port to stay up so that a device not running LACP can still connect to the network.
- The commands for applying a Media Access Control security (MACsec) profile to a port have moved from under `config switch interface` to under `config switch physical-port`. In addition, the `execute macsec clearstat interface`, `execute macsec reset interface`, and `execute macsec toggle interface` commands are now the `execute macsec clearstat physical-port`, `execute macsec reset physical-port`, and `execute macsec toggle physical-port` commands.
- A new CLI command allows you to specify which hash algorithm is used to encode passwords for new administrator accounts. You can select the PBKDF2, SHA1, or SHA256 hash algorithm. By default, the SHA256 hash algorithm is used.
- The `execute system admin account-convert` command has been changed to `execute system admin account-convert-sha1` and `execute system admin account-convert-sha256`:
 - Before downgrading to a FortiSwitchOS version earlier than 7.0.0, you need to ensure that the administrator password is in SHA1 format. Use the `execute system admin account-convert-sha1` command to convert the administrator password to SHA1 encryption.
 - Before downgrading to FortiSwitchOS 7.0.0 or later, you need to ensure that the administrator password is in SHA1 or SHA256 format. Use the `execute system admin account-convert-sha1` command to convert the administrator password to SHA1 encryption. Use the `execute system admin account-convert-sha256` command to convert the password for a system administrator account to SHA256 encryption.
- The new `set wildcard-fallback` command allows FortiSwitchOS to try to match a login name with wildcard system administrator names if FortiSwitchOS cannot match the exact login name.
- You can now split ports on the FS-T1024E and FS-1024E models. You can enable the maximum speed (100G) of ports 25 and 26; each split port has a maximum speed of 25G.

GUI and CLI changes

- FS-1xx and FS-2xx models now support configuring a DHCP server.
- You can now add multiple administrators with wildcards in their names.

REST API changes

The following REST API endpoint is new:

- The new `execute/backup/config` endpoint allows you to back up the switch's configuration.

The following REST API endpoint was removed:

- `execute/backup/standalone-config`

The following REST API schema changes were made for this release:

- In the `cmdb/router/static` endpoint, there is a new `gw-l2-switch` parameter to enable or disable the layer-2 gateway on the FortiSwitch unit.
- In the `cmdb/switch/global` endpoint, the `auto-fortilink-discovery` parameter was removed.
- In the `cmdb/switch/interface` endpoint, the `auto-discovery-fortilink` parameter was removed.
- In the `cmdb/switch/physical-port` endpoint, you can now specify `2500full` for the `speed` parameter.
- In the `monitor/switch/port-speed` endpoint, you can now specify `2500full` for the `supported_speeds` parameter.
- In the `cmdb/switch.lldp/profile` endpoint, the `auto-isl-auth`, `auto-isl-auth-encrypt`, `auto-isl-auth-user`, `auto-isl-auth-identity`, and `auto-isl-auth-reauth` parameters were added.
- In the `cmdb/switch/trunk` endpoint, there is a new `fallback-port` parameter for specifying the LACP fallback port.
- In the `cmdb/switch.acl/prelookup` endpoint, the new `interface-all` parameter allows you to select all interfaces.
- In the `cmdb/system/admin` endpoint, there is a new `wildcard-fallback` parameter to enable or disable attempting authentication against wildcard accounts if authenticating the current account fails.
- In the `cmdb/system.certificate/ca` endpoint, there is a new `Info` parameter for information about the CA certificate name.
- In the `cmdb/system.certificate/local` endpoint, there is a new `Info` parameter for information about the local certificate name.
- In the `cmdb/system/global` endpoint, there is a new `admin-password-hash` parameter for selecting which hash algorithm to use to encode the administrator password. The `fortilink-auto-discovery` and `auto-isl` parameters were removed.

Refer to the [FortiSwitch feature matrix](#) for details about the features supported by each FortiSwitch model.

Special notices

Zero-touch management

When a new FortiSwitch unit is started, by default, it will connect to the available manager, which can be a FortiGate device, FortiLAN Cloud, or FortiSwitch Manager. All ports are enabled for auto discovery. The “internal” interface is the DHCP client in all FortiSwitch models. If you do not want your FortiSwitch unit to be managed, you must disable the features that you do not want active.

By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later

After an `execute factoryreset` command is executed on a FortiSwitch unit in standalone mode, the auto-network configuration is enabled by default. If you are not using auto-network, you must manually disable it:

```
config switch auto-network
    set status disable
end
```

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading your FortiSwitchOS version requires converting the admin password format first

Before downgrading to a FortiSwitchOS version earlier than 7.0.0, you need to ensure that the administrator password is in SHA1 format. Use the `execute system admin account-convert-sha1` command to convert the administrator password to SHA1 encryption.

Before downgrading to FortiSwitchOS 7.0.0 or later, you need to ensure that the administrator password is in SHA1 or SHA256 format.

- Use the `execute system admin account-convert-sha1` command to convert the administrator password to SHA1 encryption.
- Use the `execute system admin account-convert-sha256` command to convert the password for a system administrator account to SHA256 encryption.



If you do not convert the admin password before downgrading, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

To convert the format of the admin password to SHA1 format:

1. Enter the following CLI command to convert the admin password to SHA1 encryption:

```
execute system admin account-convert-sha1 <admin_name>
```

2. Downgrade your firmware.

To convert the format of the admin password to SHA256 format:

1. Enter the following CLI command to convert the admin password to SHA256 encryption:

```
execute system admin account-convert-sha256 <admin_name>
```

2. Downgrade your firmware.

Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitchOS 7.4.0 supports upgrading from FortiSwitchOS 3.5.0 and later.

For the FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, and FS-M426-FPOE models, there is a two-step upgrade process if you are upgrading from FortiSwitchOS 6.0.x or 6.2.x to 7.2.x:

1. Upgrade from FortiSwitchOS 6.0.x or 6.2.x to FortiSwitchOS 6.4.12 or later.
2. Upgrade from FortiSwitchOS 6.4.12 or later to 7.2.x.



If you do not follow the two-step upgrade process, the FortiSwitch unit will not start after the upgrade, and you will need to use the serial console to conclude the upgrade (BIOS and OS).

For FortiSwitch units managed by FortiGate units, refer to the [FortiLink Release Notes](#) for upgrade information.

Product integration and support

FortiSwitchOS 7.4.0 support

The following table lists FortiSwitchOS 7.4.0 product integration and support information.

Web browser	<ul style="list-style-type: none">• Mozilla Firefox version 52• Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.4.0. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
829804	Changed which CLI commands are available, depending on whether the user has the enhanced debugging license.
833450	Do not use multicast IP addresses in the ranges of 224-239.0.0.x and 224-239.128.0.x on the FS-2xxD, FS-2xxE, FS-4xxD, and FS-4xxE models.
848619	When connecting FS-124F-POE to FS-148F-POE with the FTLF8519P3BNLFTN, the SFP module port does not come up on the FS-148F-POE when auto-module is configured.
856123	When the <code>network-monitor settings</code> are enabled, there are multiple "CPU_SENSOR (78.0%) cleared warning threshold of (85.0%)" messages in the log.
859563	When the admin password contains a space and is set in the GUI, the user cannot log in using the GUI.
866288	ACLs should work correctly on the FS-3032E model.
867758	FortiSwitch units using IPv6 do not respond to SNMPv3 requests.
868358	It should be optional to specify the Certificate Authority (CA) name when downloading the CA certificate using the Simple Certificate Enrollment Protocol (SCEP).
868886, 869843	The GUI for the FS-224E-POE, FS-248E-POE, FS-448E-POE, FS-248E-FPOE, and FS-M426E-FPOE models shows the ports in brown and the message, "This port is unavailable under the current configuration."
869616	The FortiAnalyzer and FortiSwitch logs have multiple entries about the fan tray being detected or undetected on an FS-1048E switch, although the fan status is good.
872727	After upgrading FortiSwitchOS, the status of PSU2 is wrongly reported as "Not inserted."
874684	Some layer-2 managed FortiSwitch units are flagged as being layer-3 switches in the output for the <code>execute switch-controller get-conn-status</code> command.
876134	The <i>Switch > Interfaces</i> page indicates that more than one security group can be selected, although only one is supported.
877360	Using one of the <code>mac-move</code> commands on FX-1xxE and FS-1xxF models causes protocol packets to be dropped when allowing an 802.1X client to move between ports that are not directly connected to the FortiSwitch unit without having to delete the 802.1X session.
878762	A VLAN interface labeled <code>mgmt</code> causes the GUI to crash frequently.
879156	Creating a new LLDP-MED profile in the GUI results in an Internal Server Error.
885609	The Web console only works with the <code>super_admin</code> profile.

Bug ID	Description
891323	Going to the <i>Router > Config > OSPF > Areas</i> page results in an Internal Server Error.
892788	After the switch is rebooted, the <code>fortilink-auto-discovery</code> setting changes from disabled to enabled.
896010	Some switches will assign two split ports with the same physical MAC address.
896288	For VXLAN interfaces, the static MAC addresses on the VLAN need to be added to the VXLAN MAC address table instead of the VLAN MAC address table.
898637	The <code>set poe-pre-standard-detect enable</code> command does not work on the FS-124F-FPOE and FS-148F-FPOE models.
902910	The 2048 key size generated certificate file shows the wrong key size in the CSR decoder.
905384	The IGMP-snooping daemon crashes on the FS-148F model.
906594	The GUI needs to support static IP/32.

Known issues

The following known issues have been identified with FortiSwitchOS 7.4.0. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANS).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	<p>When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server.</p> <p>Workarounds:</p> <ul style="list-style-type: none"> —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the <code>execute interface dhcpclient-renew <interface></code> command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	<p>The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values.</p> <p>Workaround: When using the cable diagnostics feature on a port (with the <code>diagnose switch physical-ports cable-diag <physical port name></code> CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.</p>
542031	For the 5xx switches, the <code>diagnose switch physical-ports led-flash</code> command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
572052	<p>Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters.</p> <p>Workaround: Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.</p>
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.

Bug ID	Description
606044/610149	The results are inaccurate when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
659487	The FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE, FS-148E, and FS-148E-POE models support ACL packet counters but not byte counters. The <code>get switch acl counters</code> commands always show the number of bytes as 0.
667079	For the FSR-112D-POE model: <ul style="list-style-type: none"> If you have enabled IGMP snooping or MLD snooping, the FortiSwitch unit does not support IPv6 features and cannot pass IPv6 protocol packets transparently. If you want to use IGMP snooping or MLD snooping with IPv6 features, you need to <code>enable set flood-unknown-multicast</code> under the <code>config switch global</code> command.
673433	Some 7-meter direct-attach cables (DACs) cause traffic loss for the FS- 448E model.
748210	The MAC authentication bypass (MAB) sometimes does not work on the FS-424E when a third-party hub is disconnected and then reconnected.
784585	When a dynamic LACP trunk has formed between switches in an MRP ring, the MRP ring cannot be closed. Deleting the dynamic LACP trunk does not fix this issue. MRP supports only physical ports and static trunks; MRP does not support dynamic LACP trunks. Workaround: Disable MRP and then re-enable MRP.
793145	VXLAN does not work with the following: <ul style="list-style-type: none"> log-mac-event DHCP snooping LLDP-assigned VLANs NAC Block intra-VLAN traffic
828603	The <code>oids.html</code> file is not accurate.
829807	eBGP does not advertise routes to its peer by default unless the <code>set ebgp-requires-policy disable</code> command is explicitly configured or inbound/outbound policies are configured.
867108	Depending on your browser type/version, web UI access might fail when using TLS 1.3 and client certificate authentication. Workaround: Use TLS 1.2.
916405	FortiSwitchOS should not allow MACsec and 802.1X authentication to be configured on the same port.
919990	The GUI displays a warning message of "Unverified Image Detected" when the user logs in to FortiSwitchOS 7.4.0 build 0767, even though the image is verified.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.